IBM Security AppScan Enterprise

Application security testing and risk management

Most organizations today depend on software applications to run their business processes, to conduct transactions with suppliers and to deliver services to customers. Unfortunately, in the race to stay ahead of competition, many spend little to no effort to ensure that these applications are secure. Applications can compromise the overall security of an organization by introducing vulnerabilities that hackers can use to gain access to confidential company information or customer data.

And with nearly 4,000 new web application vulnerabilities discovered every year and 92 percent of all lost data records being the result of attacks against web applications, an ad hoc or reactive approach to application security testing and remediation is clearly not enough to keep up with evolving threats. Organizations today must implement application security programs and require solutions that help integrate security testing into the software development lifecycle so that vulnerabilities can be identified and corrected before they expose the organization to new threats.

IBM Security AppScan® Enterprise software offers advanced application security testing and risk management with a platform that drives governance, collaboration and security intelligence throughout the application lifecycle. With this strategic approach to application security and risk management, IBM Security AppScan Enterprise software can help organizations:

• Reduce application risk with security testing and remediation that identifies and eliminates vulnerabilities
• Control application project costs by identifying vulnerabilities and defects early in the process

Highlights

- Perform automated security assessments of applications using sophisticated testing techniques
- Drive collaboration between security, development and testing teams by integrating development systems and tools
- Provide enterprise-level visibility of application security and regulatory compliance risks to help mitigate risk and reduce costs
- Expand security intelligence with QRadar SIEM from Q1 Labs, an IBM Company
• Monitor the progress of application security programs
• Manage regulatory demands for protecting sensitive data processed by web applications

Operationalize security testing in the application lifecycle

When security teams run pre-production tests just before the product launch, application security can become a bottleneck for the software development process. The problem has become much more pronounced as organizations now develop and run hundreds, or even thousands, of applications responsible for mission-critical processes and data. A small team of security analysts cannot keep up. Too often they end up testing only a small fraction of the total applications, and as a result, organizations face a growing risk of critical vulnerabilities that open the door to possible attacks, exploitations and data losses.

IBM Security AppScan Enterprise software offers scalability with governance and control to execute application security testing and remediation throughout the application lifecycle. Instead of executing security tests for a handful of applications, security teams can now build test scripts to be executed as part of the routine development and quality testing processes—and security experts are not needed to run these test scripts. IBM Security AppScan Enterprise provides a security testing platform to help:

• Security analysts define test policies and scan templates for development and testing organizations
• Developers execute dynamic application security testing for compiled applications using the simple Quick Scan web interface
• Developers perform static application security testing of source code in the integrated development environment (IDE) or incorporate automated security testing in the development process
• Testers run dynamic security tests predefined in IBM Rational® Quality Manager software with test cases that map to the quality plan and security requirements

With a centralized platform to execute concurrent security scans for applications in development and production, IBM Security AppScan Enterprise software can help security teams make sure that every application is tested before launch and that every application in production is scanned regularly for new threats.

Figure 1: The IBM Security AppScan Enterprise software interface provides a dashboard of application risk.
Collaborate to remediate defects and reduce risk

Identifying vulnerabilities only reveals potential risk. Organizations must then take action and correct the vulnerabilities to improve their security—but this is where many struggle. Development teams need more than just a list of security defects added to their queue. Testers need test scripts that map back to their test plans. And security analysts need to oversee the process to make sure vulnerabilities are corrected and applications are retested and launched without major risks.

IBM Security AppScan Enterprise software provides a platform to drive collaboration between security, development and testing teams. It offers a web portal for centralized results and management and integrates with the IBM Rational Collaborative Lifecycle Management solution to link security requirements to development tasks, quality plans and security tests. IBM Security AppScan Enterprise software includes collaboration features to:

- Prioritize vulnerabilities and open issues based on risk
- Assign ownership for each issue using the portal or defect tracking systems
- Track resolution
- Retest and compare results to confirm remediation

For each reported security vulnerability, IBM Security AppScan Enterprise software offers a technical explanation of the issue and the risk it introduces, plus suggested code revisions that can eliminate the vulnerability. From their IDE or web interface, developers can access the information they need to understand the vulnerability, take action to address the defect and learn how to avoid similar vulnerabilities in the future.

Monitor and manage application risk

The goal of application security testing is to identify and correct the security vulnerabilities that introduce risk. But when testing results and data obtained from tests remain isolated from those who remediate defects, organizations lack the complete view of their aggregate application risk. Once application security testing is in place, executives from security, development and compliance teams require solutions to monitor the progress over time and identify areas of concern.

IBM Security AppScan Enterprise software goes beyond security testing to provide a platform for application risk management that delivers:

- Visibility of applications and processes with an application risk dashboard
- Trending analysis and key performance indicators to monitor open issues, remediation cycles, current state of application risk and more
- Central control to cover all production applications with regularly scheduled scans
- Compliance reporting with more than 40 templates that map application security to regulations such as PCI, HIPAA, EU Data Protection Directive, Security Control Standard (ISO 27001) and more
## Engage all stakeholders throughout the software lifecycle

### Information security
- Schedule and automate assessments
- Manage test policies and scan permissions
- Facilitate collaboration between development and quality assurance teams to remediate security vulnerabilities by publishing findings to IBM Rational Team Concert™ software or other defect-tracking systems
- Devise protection strategies based on discovered vulnerabilities

### Development and build automation
- Perform automated source code analysis for security issues from IDE or as part of build verification with Security AppScan Source software
- Execute dynamic analysis of applications to test for security vulnerabilities at the end of a development iteration
- Track security defects using Rational Team Concert software or other defect-tracking systems
- Learn how to remediate vulnerabilities using built-in advisories and fix recommendations

### Quality assurance
- Link security requirements with quality plans in Rational Quality Manager software
- Execute security tests scripts in Rational Quality Manager software
- Track and manage open issues in Rational Team Concert software or other defect-tracking systems

### Management
- Gain enterprise-view of application security risk
- View trending and reporting with key performance indicators

### Compliance officers
- Review compliance reports
- Audit vulnerability resolution

*Figure 2: IBM Security AppScan Enterprise software delivers more than 40 compliance reports. This sample PCI report maps specific regulatory requirements to identified vulnerabilities while tracking resolution of those issues.*
Perform dynamic, static and hybrid analysis
IBM Security AppScan Enterprise software brings together dynamic and static analysis in a single solution and also delivers innovative hybrid analysis—the integration of dynamic and static testing—for detailed analysis and precise results. By integrating information that typically resides in separate point products, IBM Security AppScan Enterprise software drives security intelligence with actionable information that links proof-of-exploit with line-of-code details.

The modular nature of IBM Security AppScan Enterprise software enables clients to customize their solution based on their specific needs. The IBM Security AppScan Enterprise Server provides a centralized repository for all application security assessments. Clients can perform dynamic application security testing with IBM Security AppScan Enterprise Dynamic Analysis Scanner software and static application security testing with IBM Security AppScan Source software.

IBM Security AppScan Enterprise Dynamic Analysis Scanner software can be used to execute multiple concurrent dynamic analysis assessments and provide a scalable testing solution for organizations to identify vulnerabilities in their applications in the development, quality testing, pre-production testing or production phases. IBM Security AppScan Source can execute static-code analysis for security issues and can be run on a desktop client by security analysts, in the IDE by developers or automatically in the build system.

All dynamic and static test results are aggregated in the IBM Security AppScan Enterprise Server, which provides a centralized platform for security testing and application risk management. The server can correlate results from dynamic and static assessments to provide more information about the discovered vulnerabilities and suggestions for correcting them.

Figure 3: IBM Security AppScan Enterprise software provides the central platform for managing application security testing with dynamic, static and hybrid analysis that correlates the results of dynamic and static tests to provide line-of-code details with proof of exploitation.
Mitigate risk by blocking attacks with IBM security defenses

The best way to reduce the threat of attacks and data loss is to proactively address application security to identify and correct vulnerabilities. However, new vulnerabilities and threats are discovered every day. As organizations execute regular scans for their production applications, they are likely to find new vulnerabilities for hackers to exploit. When organizations identify security defects in their mission-critical applications, they need a solution that enables them to keep these applications online and protect them from attacks while they wait for their development teams to create a software patch or release a new version of the application.

IBM Security AppScan Enterprise software delivers the capability to integrate application vulnerability management with application protection strategies. It integrates with IBM Security Network Intrusion Prevention Systems to protect specific vulnerabilities with a “virtual patch.” Vulnerabilities identified by IBM Security AppScan software are published in the IBM Proventia® Management SiteProtector™ system, the central management console for the IBM Security Network Intrusion Prevention System. SiteProtector is used to correlate the vulnerabilities detected using IBM Security AppScan software with real-time network security events to effectively prioritize security issues and implement protection policies specific to the vulnerabilities. Organizations can then deploy these protection policies to block attacks targeting their applications.

Expand security intelligence with application vulnerability data

QRadar security information and event management (SIEM) collects, stores and analyzes informational data and provides real-time event correlation for use in threat detection and compliance reporting and auditing. For organizations that create millions or billions of events per day, distilling data down to priority offenses can be a daunting task. IBM Security AppScan Enterprise integrates with QRadar to provide application vulnerability data, which QRadar uses to reduce all of these events into a handful of actionable offenses prioritized according to their business impact.

In addition, application vulnerability data is provided to the QRadar Risk Manager analytics engine to enable security experts to simulate attacks, to determine the exploitability of vulnerable application assets and to gain an understanding of the risk they present to the organization.
IBM Security AppScan Enterprise solution components

<table>
<thead>
<tr>
<th>Solution components</th>
<th>Features and benefits</th>
</tr>
</thead>
</table>
| IBM Security AppScan Enterprise Server      | • Centralized platform for managing application security and risk for multiple applications  
• Collaboration between security, development and testing teams to remediate vulnerabilities and reduce risk  
• Enterprise-wide view of application security and compliance risk with more than 40 report templates for measuring compliance, trending and key performance indicators  
• Correlation and triage security testing results from dynamic (black box) and static (white box) scans  
• Integration with Proventia Management SiteProtector system, IBM Security Network Intrusion Prevention System and IBM Security Server Protection solution to block attacks that target vulnerabilities identified by IBM Security AppScan software |
| IBM Security AppScan Enterprise Dynamic Analysis Scanner | • Advanced application security testing by applying dynamic application security testing  
• Glass box testing, a form of IAST, run time analysis that applies an internal agent to monitor application behavior during a dynamic test, providing more accurate test results and identifying specific lines of code  
• Ability to run multiple concurrent scans on a single server  
• Scalable security testing to cover numerous applications by performing multiple privacy assessments of websites using dynamic analysis scanners to identify personally identifiable information collection points and verify that security safeguards are in place when collecting and transmitting customer data |
| IBM Security AppScan Enterprise Dynamic Analysis User | • Web-based user to execute security scans, triage results, collaborate with development teams, create reports and drive application risk management  
• Options for simple Quick Scan web interface for developers and testers to run test scripts designed by security analysts |
| IBM Security AppScan Enterprise Reporting User | • Web-based user to triage testing results, collaborate with development teams, create reports and drive application risk management |
| IBM Security AppScan Source                  | • Source code analysis to identify the latest security threats with static application security testing  
• Quick analysis and recommended corrections in IDE  
• Automated security testing in build environments  
• Static analysis for quality and non-security defects to improve overall code quality and predictability by identifying and resolving potential coding errors early in the software development lifecycle |

Why IBM?
IBM delivers a comprehensive portfolio of application security and risk management solutions. With advanced security testing and a platform managing application risk, the IBM Security AppScan portfolio delivers security expertise and offers critical integrations with application lifecycle management solutions that help organizations to not just identify vulnerabilities, but to reduce overall application risk. The IBM Security AppScan portfolio offers advanced static and dynamic application security testing and innovative technologies that keep up with the latest threats and drive precise, actionable results.

Application security is a core component of the IBM Security Framework. The IBM Security AppScan software family is complemented by software-as-a-service delivery options and robust professional services offerings, including application security assessments, deployment services, advanced application security training, product training and more. In addition to application security testing, IBM Security delivers application security solutions that protect against attacks and securely manage identity and access for application users.
For more information
To learn more about how IBM Security AppScan Enterprise software advanced application security testing can help drive governance, collaboration and risk management throughout the application lifecycle, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/software/awdtools/appscan

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing

© Copyright IBM Corporation 2012
IBM Corporation
Software Group
Route 100
Somers, NY 10589
Produced in the United States of America
June 2012
IBM, the IBM logo, ibm.com, AppScan, Proventia, and Rational are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.
